AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of the claims in the application:

1. (Currently Amended) A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:

receiving a request from a user of the computer system to use a piece of electronic media content;

identifying one or more software modules authorized to execute on the computer system and being responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user;

evaluating one or more predefined characteristics of the one or more identified, authorized software modules to determine if the one or more software modules are operable to process the electronic media content in an authorized manner, the evaluating including at least one protection mechanism selected from the group consisting of:

evaluating whether the one or more software modules make calls to certain system interfaces;

determining whether the one or more software modules include one or more predefined code sequences associated with undesirable behavior;

analyzing dynamic timing characteristics of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity;

determining whether the one or more software modules are included on a list of trusted software modules;

determining whether the one or more software modules are included on a list of untrusted software modules; and

determining whether the one or more software modules have been digitally signed by a trusted party; and

denying the request to use the piece of electronic media content if the evaluation of the one or more predefined characteristics fail to satisfy a set of predefined criteria.

2. (Previously presented) A method as in claim 1, further including:

using the predefined criteria to evaluate the predefined characteristics of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation.

3. (Previously presented) A method as in claim 1, in which the evaluating one or more predefined characteristics of the one or more software modules includes computing the cryptographic hash of at least one of the one or more software modules.

4. (Currently amended) A system for protecting electronic media content and enabling use of the electronic media content by a user, the system comprising:

means for applying a cryptographic fingerprint to the electronic media content;

means for evaluating one or more predefined characteristics of one or more drivers responsible for handling the electronic media content, the means for evaluating including means for operating a protection mechanism selected from the group consisting of:

means for evaluating whether the one or more drivers make calls to certain system interfaces;

means for determining whether the one or more drivers include one or more predefined code sequences associated with undesirable behavior;

means for analyzing dynamic timing characteristics of the one or more drivers for anomalous timing characteristics indicative of invalid or malicious activity;

means for determining whether the one or more drivers are included on a list of trusted drivers;

means for determining whether the one or more drivers are included on a list of untrusted drivers; and

means for determining whether the one or more drivers have been digitally signed by a trusted party;

means for denying effective access to the electronic media content based on an output of said means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic media content;

means for generating an identifier associated with the electronic media content;

means for monitoring a predefined system interface for data to be transferred to an output device and containing the identifier; and

means for preventing effective access to data containing the identifier via the predefined system interface.

5. (Currently amended) A method for protecting electronic media content from unauthorized use, the method including:

receiving a request to access a piece of electronic media content;

generating a first identifier associated with the electronic media content; and

monitoring at least one system interface for electronic data to be transferred to an output device, the monitoring including:

receiving a piece of electronic data to be transferred to the output device;

generating a second identifier associated with the piece of electronic data;

comparing the second identifier with the first identifier; and

taking a predefined defensive action if the second identifier is related to the first identifier in a predefined manner, wherein the predefined defensive action is selected from the group consisting of: modifying at least a portion of the piece of electronic data, or preventing the transfer of at least a portion of the piece of electronic data to ~~an~~ the output device via the system interface.

6. (Previously presented) A method as in claim 5, wherein the piece of electronic media content is encrypted and further including:

decrypting the electronic media content.

7. (Previously presented) A method as in claim 5, in which the first identifier comprises a hash of at least a portion of the electronic media content, and in which the second identifier comprises a hash of at least a portion of the piece of electronic data.

8. (Previously presented) A method as in claim 5, in which the first identifier comprises a predefined portion of the electronic media content and in which the second identifier comprises a predefined portion of the piece of electronic data.

9. (Original) A method as in claim 5, in which the system interface comprises a file system interface to one or more device drivers.

10. (Original) A method as in claim 5, in which the predefined defensive action comprises modifying at least a portion of the piece of electronic data.

11. (Original) A method as in claim 10, in which modifying at least a portion of the piece of electronic data includes scrambling at least a portion of the piece of electronic data.

12. (Original) A method as in claim 5, in which the predefined defensive action comprises adding noise to at least a portion of the piece of electronic data.

13. (Original) A method as in claim 5, in which the predefined defensive action comprises adding an electronic watermark or fingerprint to at least a portion of the piece of electronic data.

14. (Original) A method as in claim 5, in which the predefined defensive action comprises preventing the transfer of at least a portion of the piece of electronic data to an output device via the system interface.

15. (Original) A method as in claim 5, in which the predefined relation between the first identifier and the second identifier comprises the first identifier being equal to the second identifier.

16. (Previously presented) A method as in claim 5, in which the at least one system interface is selected using rules associated with the electronic media content, the rules being operable to identify certain system interfaces to which the electronic media content is not allowed to be sent.

17. (Original) A method as in claim 9, in which the one or more device drivers are selected from the group consisting of: video display driver, sound driver, SCSI driver, IDE driver, network driver, video capture driver, floppy disk driver, and scanner driver.

18. (Previously presented) A method as in claim 5, further including:

inserting a cryptographic fingerprint into the piece of electronic media content, the cryptographic fingerprint containing information relating to the request to access said piece of electronic media content.

19. (Previously presented) A method as in claim 18, in which inserting said cryptographic fingerprint into the piece of electronic media content includes:

authenticating a fingerprinting engine using a cryptographic credential; and

using the fingerprinting engine to insert the cryptographic fingerprint into the piece of electronic media content.

20. (Original) A method as in claim 19, in which the fingerprinting engine is operable to authenticate a calling application using a cryptographic credential.